U.S. DEPARTMENT OF EDUCATION

Information Technology Security Manual

Prepared by
ADP Security Oversight Staff
Information Resources Group
Office of Management

Information Technology Security Program
Table of Contents

Part 1 - Overview

Part 2 - The Information Technology Security Program

Part 3 - ADP Systems Security

Part 4 - Telecommunications Security

Part 4 - Telecommunications Security (continued)

Part 5 - Office Automation and Microcomputer Security

Information Technology Security Program

Policy

Part 1 - Overview

I. Introduction

A. Information processing has become a critical support system for today's government business. Managers and employees at all levels depend on and must have confidence in the information required for routine operations and major decisions. Such confidence is based upon the integrity and continuing control of information and its processing.

B. People and machines together form an information system that is highly effective and productive. However, all information systems involve certain risks that must be addressed adequately through proper controls. The policies contained in this document represent management's commitment to the security and control of the Department's information resources.

C. The arrival of EDNet (the Department's information network); the proliferation of microcomputers (PCs); and the "rightsizing" of the Department's Automated Information Systems (AIS), are all changes to the Department's information technology culture. In days past, the management of information resources, including security, was done in a centralized manner. However, partly because of the changes identified above, information resources management must, by necessity, be done in a more de-centralized approach.

D. Since Information Technology Security (formerly ADP Security) is one of the areas that must be implemented in a de-centralized fashion, it stands to reason that this area will also benefit from de-centralizing its management. This policy document is intended to form the basis for the necessary changes that will allow de-centralized management of Information Technology Security.

II. Purpose

A. The purpose of this document is to establish an Information Technology Security Program for Automated Information Systems, and to provide all employees with uniform policies for the protection and control of information resources directly or indirectly relating to the activities of the Department.

B. It is the intent of this document to promulgate only Department-wide policies. It is incumbent upon the head of each Principal Office/Service Area to supplement the contents of this document to impose more stringent standards where warranted by their particular situation.

C. Nothing in this document should be construed as superseding Federal statutes or directives. If a conflict should exist, the Federal statutes and directives shall prevail.

III. Objectives

A. The objectives of this document are to:

1. provide an infrastructure for the protection and control of information resources applicable to data automation;

2. establish policies and assign responsibilities for the development and maintenance of information technology security within the Department;

3. assist in the implementation of the various Federal laws and regulations relating to the protection of automated information resources;

4. promote the development and implementation of cost-effective security procedures and practices throughout the Department;

5. facilitate the monitoring of important security-related events and the reporting of security violations;

6. reduce future losses through a reduction in risk exposures; and

7. promote information technology security awareness and training.

IV. Scope

A. These policies apply to all automated information systems (AIS) owned by or operated for the Department of Education. The processing of national security information is not permitted on any AIS within the Department.

B. The following list represents the type of information/data that must be protected under this policy. This list is representative and should not be considered all inclusive:

1. information/data that can be used for financial gain (e.g., any data that controls the distribution of funds, including name and address authentication files);

2. information/data that controls or tracks government property;

3. information/data protected by the Privacy Act of 1974;

4. information/data that may be politically sensitive;

5. information/data that is necessary to the accomplishment of the Department's assigned mission;

6. information/data that would assist in activities against the Department (e.g., the findings of a security review could be used to help a criminal get access to information that would require protection);

7. information/data for timed release to the media (prior to the release time);

8. information/data that must be kept accurate;

9. information technology facilities (where computers and other information technology are housed) to ensure availability; and

10. information technology itself (theft of computers, especially notebooks, is big business).

V. Applicability

A. These policies are mandatory on all Principal Offices/Service Areas, employees, contractors, and others having access to and/or using the information technology resources of the Department of Education.

B. A waiver of the implementation of any policy statement contained herein must be obtained from the Assistant Secretary for Management or his/her designated representative. A request for waiver must be in writing and in sufficient detail as to permit a managerial decision. All such requests will be forwarded to and processed by the Information Resources Group (IRG). IRG will coordinate all waiver requests with all appropriate offices.

VII. Definitions

A. *AIS Computer Security Officer (ACSO)*. The AIS Computer Security Officer is designated by the Functional Manager of an AIS to be responsible for the security of the AIS.

B. *Accreditation*. An accreditation is the authorization and approval granted to an automated information system or network to process sensitive data in an operational environment. Accreditation is based on certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for adequate information technology security.

C. *Application*. An application is the system, functional area, or problem to which a computer is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and property management systems are examples of applications.

D. *Automated Information System (AIS)*. An AIS is the automated collection, processing, transmission, storage and dissemination of information in accordance with defined procedures.

E. *Electronic Bulletin Board System (BBS)*. A combination of computer hardware and software that is intended to allow two-way information sharing and one-way information dissemination in an interactive manner.

F. *Certification*. Certification is the technical evaluation, made as part of, and in support of, the accreditation process. Certification establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of information technology security requirements.

G. *Computer Security Officer (CSO)*. A CSO is an individual designated by the head of a Principal Office or Service Area to be responsible for the implementation and maintenance of the Information Technology Security Program within his/her organization. This position was previously designated the Principal Office Systems Security Officer.

H. *Critical Information*. Critical information is any information that is considered essential to the conduct of Federal programs or an agency's mission.

I. *EDNet*. EDNet is the Department's primary network facility. EDNet is managed and operated by IRG, and is comprised of a telecommunications system and many connected resources, including large computers, printers and Local Area Networks (servers). Use of EDNet allows connectivity between all Departmental information technology resources, from PC to mainframe. EDNet is the Department's information highway.

J. *Functional Manager*. Functional managers are those employees who have specific managerial responsibilities within a designated area (e.g., personnel, finance, health, property), and have functional authority over the process that has been, or is being, automated.

K. *Information Technology*. Information technology is the hardware and software used in connection with government information, regardless of the technology involved, whether computers, telecommunications, micrographics, optical imaging, or others. (OMB Circular A-130)

L. *Information Technology Installation*. An information technology installation is a collection of computing and/or communications equipment, software, and supporting personnel that has been configured to provide resources to support one or more functional objectives and is the operational responsibility of a single entity within an organization. An information technology installation may consist of one or more computers -- regardless of size. The computers may be co-located or dispersed throughout multiple buildings interconnected via communications links, channels or facilities.

M. *Information Technology Security Program Manager (ITSPM)*. The ITSPM is designated by the Director, IRG to be responsible for the overall effectiveness of the Information Technology Security Program throughout the Department.

N. *LAN/WAN Network Security Officer (LNSO)*. A LAN/WAN Network Security Officer is designated by the Functional Manager of a Local Area Network (LAN) or a Wide Area Network (WAN) to be responsible for the security of the LAN or WAN.

O. *Network Security Officer (NSO)***.** The NSO is designated by the Director, IRG to ensure the security of the Department's network resources, including EDNet.

P. *Risk*. Risk is the probability that a particular security threat will exploit a particular system vulnerability. An example of a system threat would be unauthorized access to files on the system's hard disk. An example of a vulnerability would be that there is no access control procedure in place. The risk in this example would be the chance that the vulnerability would be exploited.

Q. *Risk Analysis*. A determination of the threats to a system, identification of specific vulnerabilities to that system, and an in-depth analysis to determine the risks to that system and its information. A determination of the costs of losing and/or recovering the system and/or the information associated with it often is included, although it is optional.

R. *Risk Assessment*. A simple assessment of the general security posture of any given system, the purpose of which is to determine whether or not the system will be addressed as a sensitive system.

S. *Risk Management*. Risk management is defined as the process of determining the vulnerabilities and risks of operating an automated information system **(risk assessment/ analysis)**, and making management decisions as to the appropriate method of reducing them **(management of risk)**.

T. *Sensitive Information*. Sensitive information is any information, the **loss**, **misuse**, or **unauthorized access to** or **modification of** which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (the Computer Security Act of 1987)

U. *Sensitive Automated Information System*. A sensitive AIS is any AIS that requires protection because of the sensitivity of the information processed, stored or communicated by it. In addition, an AIS can be considered sensitive because it is critical to the Department's mission or the collective value of its components.

V. *System Manager.* System managers are those employees who are responsibility for the proper technical functioning of an AIS. System managers have authority over the day-to-day operation and maintenance of an AIS. System managers provide the Functional Managers with the automation support they require to perform their functions.

W. *System Operator (SYSOP)*. An individual assigned the responsibility for the day-to-day operation and maintenance of an electronic BBS.

Part 2 - The Information Technology Security Program

I. Introduction

A. The Office of Management and Budget (OMB) Circular A-130 establishes a minimum set of controls to be included in Federal automated information systems security programs. The Department's Information Technology Security Program (ITSP) is such a program. The Department's ITSP will include the preparation of policies, standards, and procedures which are consistent with government-wide policies to ensure that an adequate level of security exists for automated information systems whether maintained in-house or commercially. The OMB Circular A-130 directs that agencies shall:

1. ensure that automated information systems operate effectively and accurately;

2. ensure that there are appropriate technical, personnel, administrative, and telecommunications safeguards in automated information systems; and

3. ensure the continuity of the operation of automated information systems that support critical agency functions.

II. The Program

A. Organization

1. To ensure that all of its information resources are properly secured, the Department is required to establish responsibilities for individuals at all levels of management. Figure 1, Information Technology Security - Organization, provides a visual representation of the personnel with key responsibilities for the management of information technology security within the Department. These individuals are tasked with ensuring the protection of their portion (e.g., an automated information system, an IT facility, a local area network, EDNet) of the Department's information resources.

2. The responsibility for the protection of the Department's information resources not only rests on the shoulders of the personnel identified on the figure, but is shared with all personnel who operate, maintain, develop, *or use* these resources.

3. While these responsibilities are extremely important to the success of

the Department in attaining its goals and mission, they will vary from full-time duties to part-time duties depending on the complexity, sensitivity and critical nature of the information resources involved.

B. Responsibilities

1. The Information Resources Group's ADP Security Oversight Staff has been designated as the office of primary responsibility for management of the ITSP and the security of automated information, and information technology. Information technology includes, but is not limited to, computers, telecommunications equipment and software.

2. The head of each Principal Office/Service Area (PO/SA) is responsible for the protection of automated information resources within his/her jurisdiction. The head of each PO/SA also is responsible for the monitoring of information technology security within his/her jurisdiction.

3. The Functional Manager of each automated information system has overall responsibility for the security of the system that supports his/her function. Guidance for the Functional Manager is available from the appropriate security staff, the Computer Security Officer and the AIS Computer Security Officer for the particular system involved. In order to ensure that security is handled in a consistent manner which complies with all federal requirements, it is important that these sources be consulted *before* security decisions are made. Note that final decisions, and the acceptance of any risks, regarding the security of a particular system are the ultimate responsibility of the functional manager supported by that AIS.

4. Each employee of the Department is responsible for the protection of automated information resources within his/her control or possession. Guidance to assist employees is available through consultation with their Computer Security Officer or the AIS Computer Security Officer for the system being used.

C. Information Technology Security Management

1. The Director, IRG, will designate an individual, normally the Director of the ADP Security Oversight Staff, to serve as the Departmental Information Technology Security Program Manager. This individual will serve as the focal point for all matters relating to IT and data communications security at the Departmental level. The Program Manager will be responsible for the development and issuance of IT

and telecommunications security policy and guidance. In addition, the Program Manager will direct Departmental level oversight of the program.

2. The Director, IRG, will appoint an individual to serve as the corporate Network Security Officer (NSO) for all Departmental network resources, including EDNet. The specific duties of the NSO are identified in Appendix A.

3. The head of each Principal Office/Service Area will appoint an Computer Security Officer (CSO) who will serve as the focal point for IT security within the Principal Office/Service Area. This individual will provide liaison between IRG and other personnel with information technology security responsibilities within the Principal Office/Service Area. The specific duties of a CSO are identified in Appendix A.

4. The Functional Manager of each "sensitive" AIS will appoint an AIS Computer Security Officer (ACSO) who will serve as the focal point for the security of that AIS. The ACSO will assist the Functional Manager by ensuring the security of the AIS. The specific duties of an ACSO are identified in Appendix A.

5. The Functional Manager of each LAN or WAN *not under the direct responsibility of the corporate NSO*, will appoint an LNSO who will serve as the focal point for the security of that LAN/WAN. The LNSO will assist the Functional Manager by ensuring the security of the LAN/WAN. The specific duties of an LNSO are identified in Appendix A.

6. The Functional Manager of each information technology installation will designate a Facility Security Manager who will serve as the focal point for the security of the installation and be responsible for all aspects of security for the facility.

D. Planning

1. The Functional Manager of each information technology installation and automated information system will develop, with the assistance of the appropriate ACSO, an Information Technology Security Plan in accordance with the format provided in Appendix B. This Plan will be revised annually and a copy of the completed plan and each revision will be forwarded to IRG to allow for follow-up action on those items that may require it.

2. In addition, the Functional Manager must budget for periodic security reviews of his/her system. These reviews are cyclical in nature (every 3 years) and should be scheduled through the ADP Security Oversight Staff.

E. Training and Awareness

1. An Information Technology Security Training Program will be developed and implemented that will allow the Department to fully comply with awareness and training provisions of the Computer Security Act of 1987 (the Act). This program will be developed with coordination and cooperation between IRG's ADP Security Oversight Staff, the Training and Development Group's Horace Mann Learning Center and other interested offices, as appropriate. The Act specifies that each Federal agency shall provide for the "mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency." This requirement must also be complied with for all contract staff assigned to Departmental contracts.

   a. *Computer Security Awareness* The Department's Information Technology Security Training Program will provide for a suitable awareness briefing within thirty (30) days of employment with the Department. Contractor employees must be briefed within thirty (30) days of assignment to a Departmental contract. The content, frequency and documentation of these briefings must meet the requirements of the Act and the guidance of the National Institute of Standards and Technology (NIST) Special Publication 500-172.

   b. *Computer Security Training* The Department's Information Technology Security Training Program will provide for adequate training to satisfy the requirements of the Act and NIST Special Publication 500-172. The program will provide for suitable training within six (6) months of employment with the Department. The program will also provide for suitable training within six (6) months of reassignment to new duties requiring additional training.

   c. *Periodic Computer Security Refresher Briefings* The Department's Information Technology Security Training Program will provide for periodic computer security refresher briefings. These briefings will provide adequate information to ensure that personnel are kept abreast of current issues and concerns. E. Training and Awareness

F. Oversight and Evaluation

1. The ADP Security Oversight Staff within IRG will monitor, evaluate, and report annually to the Assistant Secretary for Management on the status of the ITSP within the Department and the adequacy of the activities being conducted and administered by the Principal Office/Service Area's CSOs.

2. The Principal Office/Service Area CSOs will monitor, evaluate, and report annually to ADPSOS the status of the ITSP within their jurisdiction and the adequacy of programs administered by the Installation/System CSOs.

3. Each ACSO, LNSO, and Facility Security Manager will continually monitor the status of the ITSP within their respective installation, network or surrounding their automated information system. The results of evaluations will be provided to the Principal Office/Service Area CSO where significant deficiencies are disclosed. The results will include a plan of action for the correction of the deficiencies.

4. The Principal Office/Service Area CSO will perform corrective action monitoring to ensure that corrective actions are, in fact, performed. The results of this monitoring will be reported, apart from their annual report, to the IT Security Program Manager (ITSPM) quarterly. The ITSPM will implement a program to help ensure corrective actions have been performed.

III. General Policy

A. It is the policy of the Department to comply fully with all Federal statutes and directives on automation security and to provide protection commensurate with the sensitivity of the data being processed or stored.

1. Data Ownership

a. The terms "data ownership" and "data owner" are used to indicate the party(ies) responsible for accuracy, confidentiality and availability of the data. Normally the owner of a system is its functional manager.

b. In order to establish both responsibility and accountability, owners of data will be formally designated by the head of the Principal Office/ Service Area. Designation will take the form of a memorandum from the head of the Principal Office/Service Area to the designee. A copy of this memorandum shall be forwarded to the ITSPM.

c. Designated ownership may be assigned to an organizational unit, a subordinate functional element, a position, or an individual. In those instances where ownership is assigned other than by position or individual, the head of the unit or functional element so designated shall be considered the data owner.

d. The following factors will be considered in the assignment of ownership: (1) the originator or creator of the data; (2) the organization or individual with greatest functional interest; and (3) ultimate responsibility for the integrity of the data.

e. The data owner shall be responsible for determining the sensitivity of the resources for which they are responsible.

f. The data owner shall be responsible for determining the appropriate security requirements for, and ensuring the adequate protection of, their information. All identified security requirements will be consistent with the policies prescribed herein.

g. Owners of information must consult with and give appropriate consideration to the guidance provided by their organizational and AIS Computer Security Officers.

2. Restricted Access to Information Resources

a. Access to information technology resources will be based upon demonstrated need. Individuals shall be granted only the access authority and/or system privileges necessary to accomplish their assigned duties. This restriction specifically applies to automated information systems on which sensitive information is maintained.

b. Access authorization and/or system privileges will be withdrawn immediately when such access or privileges are no longer required.

c. In the case of the Office of Inspector General's investigators, access to automated information resources will be provided once the investigator establishes the need. Such need can be established by memorandum or verbal verification by the investigator's supervisor. If verbal verification is used, an official memorandum must follow to ensure that documentation of the request and approval is available. An investigator should be allowed total unrestricted access to a automated system only when the established need specifically states it is necessary.

3. Information Technology Security Violations

a. A violation of information technology security is defined as any act resulting in:

(1) theft, fraud, or other criminal activity involving an automated information resource;

(2) unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of automated information or automated information resources; or

(3) circumvention of information technology security policies, procedures, controls, or safeguards.

b. Any individual having knowledge or suspicion of a security violation shall immediately report the incident to the CSO or the Department's IT Security Program Manager.

c. Upon notification of a known or suspected security violation, the CSO will immediately conduct a preliminary inquiry to confirm whether or not a violation has occurred; to determine the facts surrounding the incident; and to take the appropriate following action(s):

(1) promptly report to the Assistant Inspector General for Investigations any activity which may constitute a violation of law or is otherwise reportable to that office (the Assistant Inspector General will provide advice as to whether or not the local Police should be notified);

(2) promptly prepare a written report of each incident; to identify the owner of the affected resource(s), including a description of the incident and the surrounding

circumstances; identity of the persons involved; recommended corrective actions; other pertinent information; and the actions taken to prevent a recurrence;

(3) forward the original copy of the incident report to the Department's IT Security Program Manager, with copies to the Principal Office/Service Area's Security Representative;

(4) a copy of all incident reports, together with their disposition, will be retained on file for a period of three (3) years for subsequent review by the Office of Inspector General and/or the Departmental IT Security Program Manager; and

(5) all incident and investigative reports will be protected in accordance with the Privacy Act of 1974, as amended (5 U.S.C.552a).

4. Electronic Processing of National Security Classified Information

To ensure that the Department's information technology needs for future can be met without delay, a process must be identified to allow the processing of National Security Classified Information (e.g., Secret, Top Secret, Confidential) on approved AIS. This process, in the form of a procedure, must ensure that the Department's Information Security Program is fully complied with and that the Department's Information Resources Management responsibilities are also fully complied with. Close coordination will be required between the Office of Inspector General's Security Program Staff and IRG.

IV. Risk Management

A. Principal Offices/Service Areas of the Department which operate automated systems which process, transmit or produce sensitive data shall establish a program for conducting periodic risk analyses for each automated information system and information technology installation to ensure that appropriate, cost- effective safeguards are incorporated into existing and new systems. The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to a system/installation so that appropriate safeguards in the form of cost effective security controls can be effectively utilized to minimize serious potential losses. This also will have the effect of reducing the overall risk factor to an acceptable level.

B. Sensitive data will not be processed or stored on an automated information system within the Department until a risk analysis has been performed, or scheduled for the system/installation.

C. A risk analysis shall be performed in accordance as follows:

1. Prior to the approval of the design specifications for a new system/installation.

2. Whenever a significant change occurs to the system/installation (e.g., adding access to a local area network; changing from batch operations to on-line operations; installing dial-up capability; adding major features to the existing system). Criteria for defining "significant change" shall be commensurate with the sensitivity of the data to be processed, transmitted or stored.

3. At periodic intervals which are commensurate with the sensitivity of the data, but not to exceed five years if no risk analysis has been performed during that interval.

D. A satisfactory risk analysis will consist of a fully documented, formal analysis defining the vulnerabilities and threats, and the safeguards required to lower the potential loss to an acceptable level.

E. For small, stand-alone systems, the risk analysis may consist of a less detailed, but documented, analysis of the vulnerabilities, threats, and required safeguards.

F. The head of the Principal Office/Service Area will establish follow-up mechanisms to ensure that security enhancements required (and approved) as the result of risk analyses are properly installed and implemented.

G. The results of the latest risk analysis shall be considered during any evaluation of general controls over the management of information technology. These evaluations will include those that are periodically conducted in accordance with OMB Circulars A-130, A-123 and A-127.

V. Continuity of Operations

A. The concept of continuity of operations includes two distinct types of planning: (1) disaster recovery planning; and (2) contingency (or business resumption) planning.

B. **Disaster recovery planning** is the planning which an information technology installation accomplishes to ensure that, if a disaster should occur, the users of the facility are minimally impacted. This level of planning should include the following elements:

1. emergency response procedures appropriate to fire, flood, civil disorder, natural disaster, bomb threat, or any other incident or activity which may endanger lives, property, or the capability to perform essential functions. These emergency procedures will be prominently displayed in the areas to which they apply; and

2. recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at the primary site, or if necessary at an alternate facility, following the destruction, major damage, or other processing interruptions at the primary site.

C. **Contingency planning** is the planning which a *functional manager* of an automated information system accomplishes to ensure that, if the system's primary support installation cannot provide the necessary automated support services, the function can continue to be accomplished in an acceptable and timely manner. This level of planning should include the following elements:

1. arrangements, procedures and responsibilities will be defined and documented to ensure essential (critical) operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time; and

2. the minimally acceptable level of degraded operation of the essential applications or functions will be identified and prioritized to guide implementation at a back-up operational site.

D. Upon completion, each disaster recovery plan and contingency plan will be tested to the maximum extent feasible, and not less frequently than biennially thereafter. Any problems, omissions, or other deficiencies will be corrected and the appropriate portion of the plan re-tested until critical functions can be implemented within acceptable time frames.

E. All copies of disaster recovery plans and contingency plans will be maintained in a complete and current state ready for implementation at any time.

F. Disaster recovery and contingency plans will be considered sensitive, with access limited on a "need to know" basis. The information contained therein clearly could be used to the detriment of the Department if it became known to unauthorized persons.

G. A copy of all disaster recovery and contingency plans developed by each Principal Office/Service Area will be provided to the Principal Office/Service Area CSO. Current copies also will be maintained at the primary site and the alternate site selected by each preparing organization.

VI. Certification/Accreditation Policy

A. **Certification** is the process by which new software (programs/systems) is designed and verified during the development process. Certification is intended to provide assurance that the system meets all applicable Federal policies, regulations and standards, and that the results of tests performed demonstrate that the installed security safeguards are appropriate for the system.

1. Owners of *data* are responsible for determining the degree of sensitivity of the data needed to support their functions, and to specify the appropriate protection requirements. Guidance is available from Computer Security Officers.

2. Owners of *sensitive data or systems* shall define adequate security requirements in all procurement documents, and approve all security specifications prior to the start of system development.

3. Sensitive systems shall undergo rigorous design reviews and tests prior to placing the system into operation in order to ensure that all security requirements have been fully satisfied.

4. Based upon the *documented* results of the design reviews and system tests, the Functional Manager for the system will certify that the system meets all applicable Federal policies, regulations and standards and that the results of the tests demonstrate that the specified security safeguards are in-place and adequate for the sensitivity of the system being certified.

B. **Recertification**. Sensitive applications will be re-certified when substantial changes are made to the application; changes in functional requirements result in the need to process data of a higher sensitivity; the occurrence of a significant security violation raises questions about the validity of the earlier certification; and, in any event, not less than three years from the date of the previous certification.

C. **Accreditation** is the documentation of the *authorization to operate* a sensitive system. It is based on a critical review of the security requirements and components of the application; the facility it will reside on; and the entire proposed operating environment. In addition to approval for fully compliant systems, accreditation can be granted on a conditional basis.

All newly developed Departmental automated information systems that process sensitive information will receive accreditation *prior* to being placed into operational status. Although there will be no waivers to this provision, systems that were in operational status prior to the date of this policy will be allowed to seek accreditation until December 1995. Accreditation will be recorded in a letter format from the accreditation authority to the functional manager for the system undergoing review for this purpose.

D. **Certification/Accreditation Authorities**

1. Certification of a sensitive Departmental automated information system shall only be accomplished by the functional manager of the system undergoing review. The functional manager shall either unconditionally certify, conditionally certify or refuse certification. Full documentation of the reasoning behind each condition must be included in the certification letter.

2. Accreditation of a sensitive Departmental automated information system shall only be accomplished by the Senior Official of the Principal Office which the system will support. The Senior Official shall either unconditionally accredit, conditionally accredit, or refuse accreditation. For systems that have conditional certification, only conditional accreditation or refusal are acceptable. In all cases, the accreditation letter shall state the reasoning behind the choice.

VII. Contracts and Solicitations

A. It is the Department's policy to ensure that appropriate security requirements are included in solicitations and contracts for the acquisition, operation or use of AIS, (including computer facilities, equipment, and software) or for the performance of other information-related services. These requirements are necessary to safeguard AISs, sensitive information and other assets against destruction, loss or misuse.

B. This section applies to the safeguarding of sensitive information (including that which is governed by the Privacy Act), and other information resources, where non-government personnel are: (1) involved in developing AISs for use by the Department; or (2) providing any other type of service to the

Department for which information resources are used. All Department personnel who award Government funds for contractual services, where the use of information technology resources are involved, must follow the guidelines established in the Department's "*Information Technology Security: Acquisition Guideline*."

C. To be eligible for an award, offerors *must agree to comply* with the Information Technology Security Policy of the Department, as outlined in this manual.

D. **Responsibilities**

1. **Functional Managers**

a. When the issuance of an award involves the development of an AIS or the use of information technology resources, a functional manager for the involved function must be identified. The functional manager must certify that both: (1) the intent of this manual has been complied with in the procurement process; and (2) the apparently successful offeror meets the minimum acceptable security requirements of the solicitation, prior to the award of the contract (pre-award certification). These managers must work with the contracting officers or their representatives and their organization's CSOs to ensure that compliance with the Department's policies on information technology security is adequate.

b. The functional manager may authorize any qualified Department employee to perform a review of the capabilities of the offeror and recommend certification, if appropriate. The reviewer shall determine the adequacy and the capability of the offeror to meet the stipulated security requirements. To save time in the award process, reviews may be conducted simultaneously on more than one offeror.

c. In each instance of noncompliance, the functional manager shall advise the contracting officer to take appropriate enforcement action until the contractor comes into compliance with the requirements of this manual.

2. **Organizational Computer Security Officers (CSO)** shall assist the functional manager and contracting officer in carrying out the provisions of the policy. CSOs, in coordination with the appropriate contracting officer, will conduct periodic reviews of the contract to

ensure continued compliance with the requirements of this manual.

3. **Contracting Officers/Contracting Officer's Technical Representative (COTR)**. When acquisitions involve the development of an AIS or the use of information technology resources, contracting officers or their representatives must ensure that:

   a. the technical proposal instructions include a statement requiring that the offeror present a detailed outline of its proposed information technology security program and how it complies with the requirements of the solicitation and of this manual;

   b. a clause, requiring the contractor to comply with the security requirements set forth in the statement of work and this handbook is included in the solicitation. This clause must provide "flowdown coverage" of subcontractor award pursuant to the prime contract. In addition, Contracting Officers or their technical representatives are required to inform potential contractors of the *Contractor Self-Certification Program for Personnel with Low Risk ADP-Related Responsibilities* as part of the solicitation process;

   c. the functional manager has certified that the intent of this manual has been complied with in the procurement process, and that the apparently successful offeror meets the minimum acceptable security requirements of the solicitation. The contracting officer shall not issue the award until this pre-award certification, signed by the functional manager, is received;

   d. when informed by the functional manager of any instance of noncompliance, the contracting officer/COTR will take appropriate enforcement action until the contractor comes into compliance with the requirements of this manual; and

   e. copies of this manual are made available when requested by prospective offerors.

E. Contractor Self-Certification Program for Personnel with Low Risk ADP-Related Responsibilities

1. The Contractor Self-Certification Program for Personnel with Low Risk ADP-Related Responsibilities (CSCP) is a program designed to allow a contractor to "self-certify" the trustworthiness of its employees, in lieu of the government-required investigative process. This program

is applicable only to those employees whose duties have been designated as *Low Risk* by the government. Not only is this program designed to ensure the most efficient, cost-effective method of complying with Federal personnel security requirements, it also allows the contractor a degree of flexibility in regard to the utilization of its resources. This program also is intended to help increase competition for contracts by making participation easier for new contractors that do not have staff already investigated by the Government. This program is designed to ensure that: (1) the Department's contractors provide only trustworthy personnel to support and use sensitive departmental AIS; and (2) ED fully satisfies all Federal personnel security requirements.

2. It is the Department's policy to require that each of its contractors *consider* the use of the CSCP, as detailed in the "*Information Technology Security Program: Contractor Self-Certification Program for Personnel with Low Risk ADP-Related Responsibilities*." As part of their proposal submission, contractors must notify the Contracting Officer or the COTR as to whether they intend to utilize this program.

3. This program applies to all non-Federal organizations which utilize contractual vehicles to provide technical and management assistance, in the area of automation, to the Department. While compliance with this program is voluntary, it is *highly recommended* in order to promote the most efficient and cost-effective personnel screening program possible.

Part 3 - Automatic Data Processing Systems

I. Introduction

A. The establishment of a successful information technology security program is a multi-faceted challenge. Threats to a computer system are always present to some degree. They may attack the system from many different directions and locations. While these threats can never be eliminated or completely controlled, effective safeguards may be implemented to reduce their harmful effects or frequency of occurrence.

B. The policies contained in this Section are intended to provide reasonable assurance that adequate safeguards are in place and operational to protect sensitive automated information systems, networks, automation platforms and other information technology resources.

II. Physical Security

A. An effective physical security policy is an essential element of the overall information technology security program. Adequate physical security measures must be provided for the protection of human resources, physical assets, and sensitive applications and data. Physical security measures must be selected and implemented in consideration of the sensitivity of the automated information resources, and their criticality to the supported functions. The physical security policies stated herein apply to the protection of both automated information resources and all other information technology resources.

B. For the purposes of these policies, controlled areas are those which encompass or allow access to potentially sensitive information resources; resources which are essential for the processing of sensitive applications; or resources that carry a high monetary value. These areas include, but are not limited to: computer rooms; areas having terminals used to access sensitive data; data storage library; input/output area; data conversion area; programmer areas and files; documentation library; communications equipment areas; computer maintenance area; mechanical equipment area; telephone closets; environmental control and power systems; and sensitive supply storage areas.

1. The physical security requirements of controlled areas will be determined by the results of a risk analysis.

2. Where automation or data communications equipment is located

within user areas, the user management officials will assess the sensitivity of the data, the automated resources, and the functions performed and, if warranted, designate the area as a controlled area.

3. The operational areas of computer installations will be designated controlled areas to which access will not be permitted unless specifically authorized or required for job performance.

4. Controlled areas will be protected by physical security and other means which are deemed appropriate for the sensitivity or criticality of the area as determined by the results of a risk analysis. At a minimum, access to controlled areas will be limited to those individuals having an official need to be in the area.

5. Information processing devices which are easily moved, have non-volatile memory and/or non-removable hard disks, and are used for handling sensitive information will not be allowed outside of the controlled area. If the sensitive data remaining on the non-volatile media has been completely erased or obliterated, the removal of these devices from the work area may be approved by the AIS Computer Security Officer (ACSO) or the CSO.

6. Portable computers used for handling sensitive information may be removed from controlled areas provided they have adequate safeguards implemented. These safeguards can be as simple as a physical security procedure that must be followed to a third-party security software package that controls access and can provide encryption. The selection of safeguards for portable computers will bases on the sensitivity or criticality of the information or function being performed. Approval for the removal of portable computers with sensitive information stored on them must be obtained from the ACSO or CSO, as appropriate.

7. Contract maintenance personnel, and others not authorized unrestricted access but who are required to perform work in the controlled area, will be escorted by an authorized person at all times while they are within the area.

8. Media used to record and store sensitive software or data will be externally identified, protected, controlled, and secured when not in actual use.

III. Personnel Security

A. All positions that involve data processing activities of any kind may be considered sensitive to some degree. The degree will depend upon; (1) the sensitivity of the information or process associated with the position; (2) the estimated damage or loss that could be experienced should the person in the position violate a trust or act in an unauthorized or illegal manner; and (3) the technical or procedural privileges which they have been granted (or would have the expertise to exercise unilaterally).

B. All Department employees bear individual responsibility to ensure that their actions contribute to and support the required level of information technology security within their organization.

1. Procedures will be established to ensure the screening of all individuals before they are allowed to participate in the design, operation, maintenance or use of sensitive automated information systems: or are granted access to sensitive data. The level of screening required should vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and/or the risk and magnitude of loss or harm that could be caused by the individual in the course of his/her normal duties. Guidance on this subject is available in the Department's Handbook # 11, <u>Personnel Security-Suitability</u>.

2. Managers and supervisors will limit access to controlled areas and sensitive information technology resources to those personnel who are properly cleared and have a valid need for such access.

3. Managers and supervisors at all levels shall ensure that incumbents of sensitive positions attend periodic security training programs. In the absence of formal training, the manager is encouraged to develop in-house training programs to foster heightened information technology security awareness.

4. Specific technical privileges will be limited to those specifically required for job performance (e.g., a program or individual may be limited to specific data bases, utilities, programs). Privileges which have not been specifically granted will be specifically denied.

B. Where feasible, sensitive positions will be separated to preclude any one individual from gaining the opportunity to adversely affect the system. Procedural "checks and balances" must be defined and enforced so that accountability is clearly established and security violations are easily detectable.

IV. Procedural Security

A. Procedural security relates to the work flow process. Control is most easily lost at the points in the flow where processing is performed, or where control passes from one function, element, or individual to another. Procedural security is an area offering an opportunity for significant, immediate, low-cost improvement in the overall security posture of any organization.

B. Managers having responsibility for sensitive functions will develop *written* procedures to ensure that:

1. sensitive position responsibilities are delineated with defined responsibilities, privileges, and specific limitations for each individual;

2. each individual selected to fill a sensitive position will undergo security indoctrination and training designed to inform personnel of their security responsibilities, system threats, vulnerabilities, and effective countermeasures;

3. procedural controls are established to ensure that any changes to sensitive operating systems, utilities, applications, and data bases are approved, tested, and accepted prior to implementation;

4. configuration changes to the facility, hardware, communications, software, and other system or system support resources will not be implemented until the impact upon overall system security has been assessed;

5. start-up, shutdown, and system failures are handled in a safe and standardized manner, and that such events or any variations from norms are recorded and assessed for impact upon the security or integrity of the system;

6. positive controls are established over the work-flows, particularly when passing from function to function, so that an audit trail is maintained;

7. library controls (procedural, physical or logical) will be implemented to prevent unauthorized access to data, programs, or documentation, regardless of the media used;

8. plans and procedures for continuity of operations (disaster recovery and/or contingency) will be prepared; and

9. procedures to define standard responses to potential emergencies (e.g., fire, flood, wind damage, bomb threat, power outage) will be developed and prominently posted within each area in which data processing resources are located.

C. Managers will conduct periodic reviews of the security-related procedures to determine their continued effectiveness or the need for improvements.

V. Data Processing Hardware

A. Hardware-based security controls can be an important factor in creating a secure operating environment for sensitive systems. Most modern mini- and mainframe computer systems incorporate the protective features in either the hardware or software. It is not always feasible or cost effective to retrofit existing, older data processing hardware; however, the features below must be considered when acquiring new systems to ensure that they are incorporated within the hardware and/or operating system software.

1. User Isolation

a. Users will be allowed to access only the memory locations, files, and peripheral devices which have been allocated to the user by the operating system.

b. Computers should have the capability to effectively isolate users from each other and from the operating system.

c. Physical isolation of the hardware will be achieved as described in Paragraph II of Part 3 of this policy document.

2. System Execution

a. Any attempt to execute an illegal instruction should result in a hardware interrupt permitting the operating system to interrupt and abort the program containing such an instruction.

b. Error detection and memory boundary-checking should be performed on transfers of data between memory, peripherals, and external devices.

c. Automatically programmed interrupts must control system malfunctions and operator errors.

B. In addition, hardware that is to be excessed must be "sanitized" to ensure that sensitive Departmental information is not inadvertently released to the general public. This sanitization will ensure that no information or software resides on hard disks, all non-volatile memory (memory that does not lose its information when system power is removed) has been erased and overwritten, and monitor "burn-in" will not reveal any sensitive information.

VI. Software Security

A. Sensitive Applications.

1. A sensitive application requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the system.

2. Application systems development personnel will not be permitted to directly access a production software library unless a formal waiver is granted by the ACSO. Movement of application systems from test to production libraries will not be performed by development personnel. Changes or revisions will be made to software copies which shall be placed into a test library until fully tested and, if sensitive, certified and accepted.

3. New or revised application software will not be tested using sensitive data. Test files will be used until the software has been fully tested, accepted, and placed in the production library.

4. Security requirements will be defined, and security specifications approved by the user, prior to acquiring or starting development of systems/applications.

5. New or substantially modified sensitive applications shall undergo system testing prior to implementation to verify that the required administrative, technical, and physical safeguards are present and operationally adequate.

6. Sensitive system software will not be placed in a production status until the system tests have been successfully completed and the application has been properly certified.

7. System software and documentation will be afforded the security

warranted by the sensitivity of the information to be processed by the application.

8. Current copies of essential systems software, documentation, data bases, and related system resources will be maintained at a properly secured off-site location for use following an emergency.

9. Principal Office/Service Area shall perform a security audit and re-certification of sensitive systems every three years or after any significant change is made to the system or the environment within which it operates.

B. Operating Systems Software. The operating system(s) employed to process sensitive applications will contain controls which allow access only to users who have been authorized. It will contain additional controls to restrict capabilities to those that are authorized for the user. It should include means for identifying, journaling, reporting, and assigning accountability for potential compromises or violations of the system or data base security and integrity. In addition, the operating system should:

1. have access to the system software and documentation restricted to authorized personnel only;

2. be copied and stored at a secure off-site location for emergency preparedness; and

3. not be modified except as provided in this policy document.

Waivers to operating system software security requirements will be granted by the Director, Information Resources Group on a case-by-case basis. The requesting organization must document the reason for the request for waiver and forward the request to the ADP Security Oversight Staff for review and processing.

C. Utility and General-Purpose Software. Utility and general-purpose programs are available to both the operating system and the users. Many of these perform routine, but important functions for the users. Others have the capability to perform functions which may have serious security implications. Among these are the capability to by-pass controls; access data bases without the approved privilege(s); duplicate files; change or reveal passwords; and similarly inappropriate actions. When performed by an unauthorized person, such actions can compromise the protection of sensitive system resources. These latter programs will be protected by:

1. identifying those programs which are required normally only by the systems programmers. These should be password-protected and their use limited to the greatest extent practical;

2. password-protecting utilities required by the Installation/System CSO to maintain security files. Knowledge of these assigned passwords will be restricted to the designated Installation/System CSO and alternate(s);

3. limiting the availability of user instructions for these utilities to operators and others having a need for these capabilities;

4. limiting user privileges for utility and general-purpose programs to "execute only" (except for systems programmers who may need additional privileges);

5. maintaining a current copy of utilities, general-purpose programs, and documentation at a properly secured off-site location for emergency preparedness; and

6. protecting proprietary software in accordance with the terms and conditions of the contract under which the Department acquired the software.

VII. External Information Processing Services

A. Departmental automated information systems operated on another government agency's platform (computer/telecommunications system).

1. Sensitive information will be processed only on computer systems having appropriate security protection. These systems normally will be certified to handle such information by the owner of the computer system or the Designated Senior Official for Information Resources Management of the servicing organization. Based upon an evaluation of the certification and accreditation documents for the system, by the CSO, the appropriate official of this Department may then accredit the operation of the Department's AIS on the computer system.

2. If, at any time, the CSO determines that the servicing organization is not maintaining an appropriate level of security, he/she must notify the owner of the AIS/data with the recommendation to terminate the agreement.

3. Copies of the accreditation certificate of the outside organization, and any relevant correspondence, will be maintained by Head of the Principal Office/Service Area owning the data.

4. Re-certifications of sensitive systems or applications must be accomplished by the external organization at least every three years. The agreement with the organization should state that the re-certification will be accomplished, as required, and that a copy of the re-accreditation certificate will be provided to the Head of the Principal Office/Service Area owning the data.

5. It is the responsibility of the Department's data owners to determine the level of sensitivity of the data to be processed by the external organization. The security requirements will be made known to the external organization at the beginning of negotiations.

6. Employees who will have access to Departmental sensitive data at the external site must be screened in accordance with the Federal Personnel Manual (Sections 731 and 732) as implemented by the Department's Handbook #11, Personnel Security-Suitability. Any agreement between this Department and the servicing organization should contain provisions to ensure that appropriate screening will be successfully completed before access to the Department's sensitive data can be granted.

B. Departmental automated information systems operated on a Non-Government agency's platform

1. Non-Government information processing organizations, including contractor personnel, will be required to observe the security policies and maintain the same standards of security expected of Department organizations.

2. Before entering into an agreement to process or handle sensitive information at a contractor facility, an appropriate security inspection (risk analysis) of the facility will be made, and the results made available to the IT Security Program Manager.

3. The monitoring of contractor compliance with Departmental information technology security policies will be the responsibility of the COTR, in coordination with the appropriate procurement and information technology security officials.

VIII. Malicious Software Policy (Viruses)

A. Malicious software, such as computer viruses and other destructive programs, represents an increasingly serious security problem for the type of computing environment maintained by the Department. Such software often is written as independent programs that appear to provide useful functions but, in fact, they contain malicious programs that can be very destructive.

B. Viruses, for example, can spread quickly through software and data that are shared among users. Networks are particularly vulnerable because they can allow viruses to spread rapidly to all systems connected to the network. The Department's emphasis on sharing data and its increasing dependence on networked automated information systems, microcomputers (PCs), and office automation systems increases our susceptibility to viral attacks.

C. It is Departmental policy to protect information resources from unauthorized alteration, disclosure, or destruction. This includes providing a reasonably risk-free environment by minimizing the likelihood that viruses and other malicious programs will be introduced, insuring the timely detection of these types of programs; and providing reliable procedures for eliminating viral infections and other malicious programs from personal computers and networks. The following policies are intended to provide the necessary environment:

- No privately owned software/utilities will be used on the Department's computers without specific authorization from the Director, IRG or his designate. Requests for authorization shall be made, by memorandum, through the employee's supervisor/manager and CSO. Each request must provide a detailed justification for the need.

- Use of pirated software (unlicensed copies) is strictly prohibited.

- The playing of computer games on the Department's computers is strictly prohibited.

- Storage Media (e.g., floppy disks, magnetic tapes, CD-ROMs) that leave the Department's official work-space, will not be reintroduced into the Department without authorization by the CSO. The CSO shall carefully check the media to ensure that it is free of viruses and other malicious software before authorizing its use. This requirement includes all back-up media, whether or not it leaves the Department's official work-space.

- The use of software that has been downloaded from bulletin boards will only be permitted after it has been thoroughly checked by the employee's CSO to ensure that it is safe to use on the Department's computers. Downloading software from bulletin boards shall be restricted to copying to a floppy disk and not to the computer's hard disk.

IX. Security of Electronic Bulletin Board Systems

A. It is the Department's policy to promote the use of information technology in the dissemination of information to the public. It is also the Department's policy to ensure that only non-sensitive information is disseminated through Departmental BBSs, and that all Departmental BBSs are adequately protected to ensure that only appropriate usage is allowed. This policy governs the use of BBSs as information dissemination tools, and does not address electronic mail issues involved in BBS usage.

B. This policy applies to all federal and non-federal personnel involved with the operation, maintenance and use of any BBS used to conduct federal business for the Department.

C. The Principal Officer of each Principal Office that sponsors a BBS shall ensure that a SYSOP is identified and tasked with implementation of security for the BBS. In addition, the Principal Officer shall ensure that proper precautions are implemented that will ensure that only authorized information is provided to the public through the use of the BBS, and that the BBS is only used for the purpose it was intended to fulfill.

D. The SYSOP for each BBS shall serve as the BBS's application computer security officer (ACSO) and be responsible the day-to-day security of the BBS. The sysop shall also be responsible for ensuring that only authorized information is posted on the BBS for dissemination to the public.

E. The SYSOP for each BBS shall ensure that:

1. no sensitive information will be allowed on the BBS if it is accessible by the public;

2. if a sensitive BBS is absolutely necessary, *all* users have a "need-to-know" all of the information and that they have received the proper background screening;

3. every method available is used to ensure that the users of a BBS are restricted to authorized BBS functions only. There should be no

method available for a user to "break out" of the BBS and gain access to the host computer system;

4. all entries to be posted on the BBS, excluding E-mail, are reviewed to ensure no violation of law or federal directive could take place (e.g., release of information protected under the Privacy Act);

5. all entries to be posted on the BBS, excluding E-mail, are attributable to someone, and that the name and phone number are published with the entry;
6. all posted items shall be protected from unauthorized alteration; and

7. use of the BBS shall be audited frequently to ensure adequate and appropriate usage.

F. To aid in ensuring that Departmental BBSs are only used for "official" purposes, each BBS shall have a "banner page" that describes appropriate usage and penalties (loss of access rights) in case of violation.

G. A documented "clearance" procedure shall be established to aid the SYSOP in ensuring that only authorized information is posted on BBSs accessible to the public. This procedure shall include identifying the source of the information, and who authorized its posting (release) on the BBS. Each SYSOP may determine the procedure for his/her BBS. However, all procedures must be documented and approved by the Head of the Principal Office or Service Area sponsoring the BBS.

H. If a database is to be posted for public use, the database of information must be reviewed prior to its being posted on the BBS. However, refreshing the information on the database does not require a new review unless there is a change to the data elements which would actually change the information content. For example adding like records to a previously reviewed database would not require a new review, changing a data field (today's date to birth date) would.

I. All databases must be attributed to the organization that developed or is responsible for the information they contain.

Part 4 - Telecommunications Security

I. Introduction

A. Today's information technology resource environment involves the merger of computer and communication technologies. The advent of multi-user computer systems and the ability to communicate over long distances has provided the functional user with direct access to their automated information and that of others. Along with an increased productivity, increased connectivity and expanded levels of interoperability have introduced increased vulnerabilities. The policies cited below address these vulnerabilities, and are essential to the overall information technology security program.

B. The policies stated in Part 4 *do not* apply to national security information.

II. Transmission of Sensitive Data

A. The designated owner of sensitive information shall establish and periodically, at lease annually, review his/her communications security requirements in consultation with the Principal Office/Service Area CSO.

B. Encryption shall be considered where confidentiality or integrity (fraud protection) of sensitive information is of primary concern. All encryption devices shall employ the Data Encryption Standard (DES), as set forth in FIPS PUB 46, or COMSEC TYPE II devices as approved by the National Security Agency, unless a formal waiver has been granted by the Department of Commerce.

C. Management procedures pertaining to key generation, key distribution, key storage, and key destruction shall be developed and submitted to the ADP Security Oversight Staff, IRG, for review and approval prior to implementation.

D. Appropriate physical security, as defined by the provider, shall be implemented for the protection of the cryptographic devices, keys, material and information at all times.

III. Electronic Funds Transfer

All departmental systems linked to the Department of Treasury payments and/or collections system will properly authenticate all electronic funds transfers, as required by Treasury Directive 81-80, "Electronic Fund and Securities Transfer

Policy -- Message Authentication."

IV. Support of Critical Departmental Functions

Communication facilities used in support of critical functions will be assessed on a periodic basis, and alternative back-up facilities or methods for communication will be identified to assure continuity of operations. Alternative communication facilities will provide, or be capable of providing, the same degree of security as the primary facility.

V. Dial-up Telecommunications Facilities

A. Dial-up communication facilities will be used only when the need has been established and the appropriate level of security has been provided. This includes the use of dial-up communications for public outreach programs (they are not prohibited, but do require prior approval by the Director, IRG or a designated official).

B. Telephone numbers for dial-up communications will be controlled, and provided only to authorized users. Such telephone numbers will not be publicly listed or otherwise made available to the general public.

C. The use of terminal identification, call-back, encryption, and other devices/methods shall be used when deemed necessary to control access to automated information systems through dial-up communications facilities.

D. Appropriate controls will be implemented to preclude communication ports from remaining open and attached to a processor following either a normal or abnormal termination of the communication link.

VI. Network Security

A. Designated owners of information transmitted over any communications network, including LANs, will communicate their security requirements to the network owner or the NSO/Local NSO and will ensure that the requirements are implemented.

B. The network owner shall establish and maintain a level of security necessary: (1) to adequately control network access; (2) to ensure the protection and integrity of message traffic as required by the owners of the information being transmitted; and (3) to ensure the adequate protection of network nodes.

C. The NSO/Local NSO shall assist the network owner in all aspects of security related to the network. In addition, the NSO/Local NSO shall monitor the condition of security on the network to ensure that a constantly secure environment is provided for users.

D. An information technology resource will not be connected to any network, either internal or external to the Department, that does not provide adequate protection for the information transmitted or the data system so connected.

E. The use of "wireless" networking technologies demands special security requirements. This technology is easily intercepted and can be disrupted with little effort. Because of these vulnerabilities, the use of wireless networks must be approved by the Director, IRG, *prior* to implementation. The request for approval must include a detailed statement of the security impact of disruption of service or compromise of the information involved and any safeguards that will be implemented.

VII. Privacy of Electronic Mail (E-Mail)

A. The Department's electronic mail system (E-mail) is intended for the use of authorized users in the conduct of official government business only. To protect E-mail from unauthorized use and to ensure that it is functioning properly, system administrators must monitor the activity on the system. Individuals using E-mail without authority, or in excess of their authority, are subject to the monitoring of all their activities on the system and the recording of those activities by system personnel. In the course of monitoring individuals improperly using E-mail, or in the course of system maintenance, the activities of authorized users may also be observed. Anyone who uses the Department's E-mail system expressly consents to this monitoring and is advised that if the monitoring reveals possible misuse of the system or criminal activity, system personnel may provide the resulting evidence to Departmental officials responsible for personnel actions or to law enforcement officials, if appropriate.

B. The Department has taken limited measures, such as mandatory passwords, to protect communications on E-mail. However, the Department's E-mail system was not designed with the safeguards necessary to *assure* privacy or the security of sensitive information. Thus, the Department cannot guarantee, *nor should users assume*, that communications on E-mail are private/confidential. Because of the lack of protection available, the transmission of sensitive information via Departmental E-mail is not permitted unless specifically authorized by the information owner.

VIII. Identification and Authentication

A. Positive identification and authentication of authorized users of remote processing facilities will be made through the use of effective password systems.

B. The standards contained in FIPS PUB 112, "Password Usage," are adopted as the minimum standards for the Department and will be fully implemented subject to technical capabilities of the hardware. More stringent standards for password system design, operation and management may be established by a Principal Office/Service Area, as warranted.

IX. Terminal Security

A. The use of terminal equipment is on the decline within the Department; however, the security of these devices must be addressed until they no longer exist.

B. Managers and supervisors at all levels will establish appropriate procedures to control the access to, and use of, terminal equipment within their respective offices.

C. The transfer of sensitive information from a central computer to any device having the capability to record information on magnetic or other media, will not be permitted without specific authorization from the owner of the information involved.

D. Microcomputers (PC), word processors, and terminals will not be left unattended or unsecured while connected to a central computer, communications network, or similar device.

X. Access to Data Communications Facilities

A. Access to communications controllers, wiring closets, frame rooms, concentrators, processors, diagnostic equipment and circuits will be restricted to authorized personnel.

B. Reasonable care will be taken in the placement of cables forming a part of the communications distribution system in order to deter accidents, deter tampering and preclude possible loss of data and/or the ability to communicate.

XI. Documentation

The design and configuration of all data communication facilities will be fully documented by the resource owner. Such documentation, including cable plant diagrams, will be maintained on a current basis with access limited to authorized personnel only.

XII. Facsimile (FAX) Security

A. The Department's FAX equipment is intended for the use of authorized individuals in the conduct of official government business only. General-use FAX equipment is not designed to provide any reasonable level of security. There is no way of knowing, for example, if the information being sent, or received, is appropriate. In addition, there are no safeguards in the equipment to preclude individuals other than the intended recipient from reading the information.

B. Principal Offices and Service Areas that utilize this technology must develop and publish procedures that: inform users of the inherent vulnerabilities in the use of this equipment; ensure that the equipment is only used for official government business; ensure that only the intended recipient can receive the document; and that only appropriate information is transmitted.

C. Because of the lack of security safeguards, general-use FAX equipment shall not be used to transmit or receive sensitive information unless specifically authorized by the owner of the information involved.

Part 5 - Office Automation and Microcomputer Security

I. Introduction

A. The expanding use of microcomputers (i.e., PCs) and word processors in the office has placed increasingly powerful information technology in the hands of a growing number of users. While providing many benefits, the use of such systems also introduces potentially serious security risks. To ensure effective protection of these resources and capabilities, managers and users must be aware of the vulnerabilities which exist and the controls which should be applied.

B. For the purposes of this document, micro- or personal computers, on-line user terminals, and word processors will be considered under the broad term of "office automation."

C. Not all of these policies will necessarily apply to every situation. Thus, it is intended that each manager of office automation capabilities consciously evaluate and assess the need for each policy based upon a current risk assessment.

II. Physical Security

A. Most office automation equipment has utility in both the office and the home. Therefore, controls must be established and enforced to prevent, deter, and detect the misappropriation of this equipment for unauthorized purposes. Office automation devices will be secured and protected as specified by the appropriate policies and directives of the Quality Workplace Group.

B. Information technology which is easily moved, has non-volatile memory and/or non-removable hard disks is considered target equipment. Target equipment that is used for sensitive information will not be allowed outside of the area controlled by the Department for maintenance. The intent of this requirement is to avoid inadvertent disclosure of sensitive information that may reside on the non-volatile media. Target equipment may be removed if the sensitive data remaining on the non-volatile media has been adequately over-written. The removal of these devices from the work area must have prior approval of the appropriate CSO.

C. Information processing devices used for sensitive or critical information should be placed so that they are in view of office personnel at all times. If these devices cannot be placed in such a way, they must be provided with other safeguards that will ensure that unauthorized personnel cannot easily use them for any purposes.

D. Portable computers used for handling sensitive information may be removed from controlled areas provided they have adequate safeguards implemented. These safeguards can be as simple as a physical security procedure that must be followed to a third-party security software package that controls access and can provide encryption. The selection of safeguards for portable computers will bases on the sensitivity or criticality of the information or function being performed. Approval for the removal of portable computers with sensitive information stored on them must be obtained from the ACSO or CSO, as appropriate.

E. PCs, word processors and other office automation equipment on which sensitive or critical information is permanently maintained, and not located within a controlled access area, should be equipped to preclude unauthorized activation (e.g., keyboard lock, removal of keyboard).

III. Personnel Security

The personnel security policies and requirements are the same for users of office automation as they are for users of other information technologies. These policies are addressed in Part 3, above.

IV. General Policy

A. When feasible, information processing devices which handle sensitive information will be capable of identifying users through automated identification and verification techniques.

B. Access to sensitive applications, files, and records will be limited to those individuals who are properly cleared and have an established "need to know."

C. Access rights to software and information will be defined and authorized by the owner of the resource (information or software).

D. Where feasible, automatic application execution will be employed by presenting identified users with a limited menu of applications to which the user is authorized access, and no more.

E. File encryption should be considered for particularly sensitive information residing on fixed disks or in non-volatile memory (e.g., memory that maintains its contents after power has been removed). When this option is used, great care must be taken to ensure that re-encryption of the information will not be possible, whether deliberate or inadvertent.

F. If unique passwords are issued to each individual authorized to process or access sensitive information, those passwords will be constructed, assigned, used and managed in accordance with FIPS PUB 112, "Password Usage."

G. Sensitive information stored on removable media will be appropriately secured when not in use. As a minimum, the media will be marked externally to indicate its sensitivity, subject, and its owner.

V. Procedural Security

A. Formal procedures can be the most effective and economical aspects of an effective security program, providing such procedures have been carefully prepared to enhance security and that they are enforced. Such procedures are particularly important for office automation users since they represent a group of individuals who frequently have had little experience or training in information technology security matters. This situation creates a serious potential for compromise, loss, or the unauthorized modification of critical or sensitive information assets.

B. Standard procedures define the authorized actions to be performed in various circumstances, and are invaluable for training new employees as to how to avoid unintentional problems or to recover from these problems if they should occur. They also assist the manager in detecting procedural deviations which could signal the need for corrective actions ranging from additional training to disciplinary action. Formal procedures should be developed with these objectives in mind.

C. Stand-alone PCs and PCs with the capabilities to access a network shall be controlled procedurally to protect the security of the most sensitive information resources accessible from that computer.

VI. Data Communications Security

Data communications is often used in today's office automation environment. It is becoming more common to interconnect personal computers and word processors through local area networks and to provide access to central computer facilities. The policies contained in Part 4, Telecommunications, above will apply in such instances.

VII. Software Security

The software (programs) for office automation equipment, such as PCs and word processors, is often purchased from a vendor, and is normally copyrighted and licensed for the exclusive use of the purchaser. It is the policy of this Department that the terms and conditions of all license agreements be complied with fully at all times. In no instance will copyrighted software be copied or otherwise used in a manner that would violate the license agreement or the owner's copyright. In addition, the use of pirated software is strictly prohibited. All of the Department's supervisors are responsible to ensure that this policy is implemented and complied with by the employees reporting to them.

Part 6 - References, Laws and Regulations

The following list of documents, while not all inclusive, represents the body of information that this policy document was developed from.

- Office of Management and Budget, Circular A-130, "Management of Federal Information Resources"

- Office of Management and Budget, Circular A-127, "Financial Management Systems"

- Office of Management and Budget, Circular A-123, "Internal Control Systems"

- Office of Management and Budget, "Internal Control Guidelines"

- 5 CFR 950, Training Requirement for the Computer Security Act, Office of Personnel Management

- Computer Security Act of 1987, Public Law 100-235

- Federal Managers' Financial Integrity Act of 1982, Public Law 97-255

- Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a

- Computer Matching and Privacy Protection Act of 1988, Public Law 100-503

- All National Institute of Standards and Technology Federal Information Processing Standards (FIPS) publications

- National Security Telecommunications and Information Systems Security Instructions No. 4009, "National Information Systems Security (INFOSEC) Glossary"

Appendix A

Duties and Responsibilities

Computer Security Officer (CSO):

> A CSO is an individual designated by the head of a Principal Office or Service Area to be responsible for the implementation and management of the Information Technology Security Program within his/her organization.

The primary function of a CSO is to *manage* the Department's Information Technology (IT) Security Program within his/her Principal Office/Service Area. CSO duties will include, but not be limited to, the areas listed below. While each of these duties must be addressed by each CSO, the amount of time required will vary from organization to organization.

The CSO will:

- serve as the single point-of-contact within the Principal Office/Service Area for all IT Security matters;

- serve as liaison between the ADP Security Oversight Staff and other personnel responsible for ADP security activities;

- ensure that the Functional Manager for <u>each</u> automated information system within the CSO's organization is aware of his/her IT security responsibilities;

- support all levels of management within his/her organization in required IT security planning and budgeting;

- provide Information Technology Security Awareness training throughout his/her organization;

- review all ADP procurements to ensure that IT security is adequately addressed;

- monitor, evaluate and report annually to the ADP Security Oversight Staff the status of the Information Technology Security Program within their organization and the adequacy of programs administered by AIS Computer Security Officers;

- facilitate the establishment of the ownership of all data, software and hardware within his/her organization;

- ensure the reporting of and, as needed, facilitate the resolution of internal information technology security violations;

- ensure the performance of a risk analysis for each information technology installation and AIS within his/her organization;

- ensure that the requirements for Continuity of Operations Planning are complied with for each information technology installation and AIS within his/her organization;

- ensure that requirements in each of the following areas are complied with for each information technology installation and AIS within his/her organization:

  Physical Security
  Personnel Security
  Procedural Security
  Hardware Security
  Software Security

- ensure compliance with the Department's ITSP for all external information processing activities (e.g., cross-servicing), whether operated by or for the government;

- assist the Corporate Network Security Officer in ensuring that the security of the Department's network resources (EDNet) is maintained within his/her organization;

- support AIS computer security officers, as required, in their:

  maintenance of security profiles;
  participation in security reviews;
  oversight of security for individual installations/systems;
  development of system access authorizations;
  identification of system specific security problems and requirement;
  other areas as necessary.

- maintain a current list of information technology installations and AIS under his/her organization and forward it and any related documentation to the ADP Security Oversight Staff, upon request;

- take the lead in the implementation of the Department's IT Security Certification/Accreditation process;

- perform other functions that may be required to ensure the integrity, confidentiality and availability of the Department's IT resources.

AIS Computer Security Officer (ACSO):

> The AIS Computer Security Officer is an individual designated by the Functional Manager of an AIS to be responsible for the security of that AIS.

The primary function of an ACSO is to implement the Department's ITSP as it applies to the AIS and the information that it processes or stores. The ACSO shall work in close coordination with the CSO and the AIS' Functional Manager. ACSO duties will include, but not be limited to, the areas listed below. While each of these duties must be addressed by each ACSO, the amount of time required will vary from system to system.

- implement IT security for the assigned AIS;
- serve as the single point-of-contact for all IT Security matters that concern the AIS;
- serve as liaison between the CSO and other personnel responsible for IT security activities, including the Functional Manager of the AIS and owners of data, software and hardware if other than the Functional Manager;
- ensure that the Functional Manager for the AIS is aware of: (1) all matters that address the security of the AIS; and (2) his/her IT security responsibilities;
- continually monitor the status of the IT Security Program within their respective AIS and, where significant deficiencies are disclosed, provide the results of evaluations to the CSO. The information provided to the CSO shall include a plan of action for the correction of the deficiencies including target dates;
- report information technology security violations to the appropriate CSO;
- perform risk analysis for his/her assigned AIS;
- assist all operations personnel in the completion of all necessary security functions;
- maintain a security profile of the AIS;
- participate in all security reviews of the AIS;
- develop AIS specific access authorizations; and
- perform other functions that may be required to ensure the integrity, confidentiality and availability of the AIS.

Information Technology Security Program Manager (ITSPM):

The ADP Security Program Manager is designated by the Director, IRG to be responsible for the overall effectiveness of the ITSP within the Department. The ITSPM is responsible for establishment of policy and guidance to ensure that confidentiality, integrity and availability of the Department's IT resources. In addition, the ITSPM is responsible to ensure appropriate oversight of the Department's ITSP.

LAN/WAN Network Security Officer (LNSO):

A LAN/WAN Network Security Officer is designated by the Functional Manager of a Local Area Network (LAN) or a Wide Area Network (WAN) to be responsible for the security of the LAN or WAN. As a minimum, the LNSO will:

- control access to the LAN/WAN through the use of user accounts and passwords;

- develop and issue any necessary security procedures relevant to the secure operation of the LAN/WAN; and

- continually monitor and report to the CSO the security posture of the LAN/WAN.

Network Security Officer (NSO):

The NSO is designated by the Director, IRG to ensure the security of the Department's network resources, including EDNet.

The primary function of the NSO is to ensure that EDNet, and any future network, is operated and maintained in a manner that promotes the security of all information assets attached to it, including all AISs. NSO duties will include, but not be limited to, the areas listed below.

- serve as the single point-of-contact for all IT Security matters that concern EDNet;

- serve as liaison between EDNet operational and management personnel and other personnel responsible for ADP security activities, including the Director, IRG;

- ensure that the Director, IRG is aware of all matters that address the security of EDNet;

- establish security-related standards that address the minimum level of security that must be attained prior to attaching new hardware or an AIS.

Appendix B

Information Technology Security Plan Format

I. EXECUTIVE SUMMARY

[This section should summarize the review. It should include a general categorization of the adequacy of the security environment surrounding the application or facility. It also should include an identification of the system's most serious IT security deficiencies.]

[This section should not exceed one page and should be separated from the main body of the report.]

II. SYSTEM IDENTIFICATION

A. Responsible Organization U. S. Department of Education

Internal Agency Name: (e.g., Office of the Secretary)

Operating Organization:

The name of the component/office responsible for the system. If a State or local government or contractor is actually performing the function, identify BOTH the Federal and other organization AND describe the relationship.

B. System Name/Title

The name or title of the system (both full text and any acronym whenever possible).

C. System Category

Identify whether the system is a Major Application OR a General-Purpose ADP Support System. Include any explanations necessary to assure understanding.

Major Application Systems are systems that perform clearly defined functions. These systems generally have clearly identifiable security considerations and needs. Such a system might actually comprise many individual application programs and hardware, software, and telecommunications components at more than one site. Examples might include: a major agency benefits payment system or a group of systems all supporting a specific agency program.

General-Purpose ADP Support Systems consist of hardware and software that provide general ADP support for a variety of users and applications. Individual application systems are less easily distinguished than in the previous category, but such applications may contain sensitive data. Even if none of the individual applications is sensitive, the support system itself could be considered sensitive if it provides critical support for the mission of the Department. Several types of systems may be included in this category. For example, an agency computer center, facility or site; an Department-wide data network, a local area network and a grouping of personal computer work-stations, perhaps, connected by a local area network.

D. System Operational Status

Identify whether the system is Under Development, Operational, OR Undergoing Modification. Include any explanations necessary to assure understanding.

E. General Description/Purpose

1. Level of Aggregation - Identify whether the system is comprised of a single computer OR is made up of a group of computers having sufficiently similar characteristics and security requirements as to be managed and reportable as a single system. Include the number of aggregated computers (e.g., System X is comprised of 12 microcomputers).

2. Operating Environment - Identify the general operating environment of the system.

3. Description - Provide a detailed general description of the function and purpose of the system. The description should include the physical and operational environment in which the system operates. The location, types of users served or other special considerations should be described. If an application makes substantial use of a data processing facility outside the direct control of the Department, this should be indicated. Similarly, if a general ADP support system (e.g., a data center) serves a substantial external (non-agency) customer base, this should also be indicated.

F. System Environment and Special Considerations

Provide a detailed description of the technical aspects of the system. The description should include the physical, operational, and technical environment in which the system operates. Include any environmental factors that cause special security concerns (e.g., it is located in a high-crime area; software is rapidly implemented; it operates on an open network used by the general public or with overseas access; the application is processed at a facility outside of the Department's control; the general support mainframe has dial-up lines).

G. Information Contacts

Name, Title, Telephone Number and Organization of one or more federal employees within the Department and the Office designated to act as the point of contact for the system. The designated person(s) should have sufficient knowledge of the system to be able to provide reviewers with additional information as needed. Additional technical and/or contractor contacts should be included, as appropriate.

III. SENSITIVITY OF INFORMATION

A. Applicable Laws or Regulations Affecting the System

1. General Description of Information Sensitivity - Identify all of the applicable categories that describe the nature of the information handled by the system. The categories should provide the basis for the system's security requirements.

2. Applicable Laws or Regulations - List any laws or regulations that establish specific requirements for confidentiality of the information on the system (e.g., Mission Critical and P.L. 308, Financial Management and Title 29 CFR 29 & 30 and the Privacy Act). Include any other laws that may establish specific requirements for the general security of the information and/or the system.

B. General Description of Information Sensitivity

[The purpose of this section is to indicate the type and relative importance of the protection needed for the various types of information handled by the system.]

TYPE OF INFORMATION: Describe the information handled by the system and the need for protective measures. Include a description of the amount of harm that could result from the loss, misuse or unauthorized access to, or modification of, the information handled by the system.

System Protection Requirements - Certain types of information may need protection for one or more of the reasons listed below. Check all categories that apply:

- **Confidentiality -** The System contains information that requires protection from unauthorized disclosure. Examples include: For Official Use Only, timed or controlled dissemination (e.g., crop report data), personal data (covered by the Privacy Act), confidential (proprietary) business information.

- **Integrity -** The System contains information which must be protected from unauthorized, unanticipated or unintentional modification. Example: Financial transactions systems or systems critical to safety and/or life support.

- **Availability -** The System contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid other types of losses. Example: Financial Management, Operational Control, or Program Monitoring Systems.

and for each category indicate if the protection required is:

- **HIGH -** a protection requirement that has been determined to be a critical concern to the System.

- **IMPORTANT -** a protection requirement that has been determined to be an important concern, but not necessarily paramount in the organization's priorities.

- **LOW -** a protection requirement where some minimal level of security is required, but not to the same degree as the high or important categories.

IV. SYSTEM SECURITY MEASURES

A. Applicable Guidance

To the extent practical, indicate specific standards or other guidance used in the design, implementation or operation of the protective measures used by the system (e.g., relevant Federal or industry standards).

B. Management Controls

Status of Security Control Measures - For each Security Control listed, indicate the status of that control as being:

- **In Place -** the control measure of the type described is in place and operational.

- **Planned -** the control measure is planned for the system. Must give date measure is to be operational.

- **Not Applicable -** this type of control measure is not needed or inappropriate for this system.

Assignment of Security Responsibility - For each computer system a Federal employee must be assigned the responsibility for the security of the system. The name of the Federal employee assigned this security responsibility for this system, will need to be provided.

Risk Analysis - A Risk Analysis consists of a structured approach to identify assets; determine threats and vulnerabilities; estimate potential impacts; and identify effective controls for use. Include the name of any automated or formalized manual methodology used. If a risk analysis was performed, attach a copy to this report.

Formal Risk Analysis - must be conducted by persons independent of the system/facility users and management, and is commensurate with the sensitivity and scope of the data contained or processed.

Other Form of Risk Analysis - may be conducted by the system/facility users and management, and includes a checklist of recommended controls designed for the particular environment, or other acceptable methods which ensure that the system possesses appropriate safeguards.

Personnel Selection/Screening - Personnel selection/screening is required to assure an adequate level of security for Federal automated information systems. All individuals participating in the design, development, operation, or maintenance of sensitive applications MUST be screened to assure suitability. Personnel security policies and procedures should be in place that limit access to, and processing within, the application system. Only those with a documented need for access should be allowed access to the system. Describe the processes used to ensure that personnel security is effectively addressed.

C. Development Controls

[These are procedures to assure protection is built into the system, especially during system development. Even in an operational system, development controls should be addressed as a historical security measure when possible, and as an ongoing measure to control hardware and software modifications. OMB Circular A-130, Appendix III, Section 3, provides guidance in this area. These controls may also include any software configuration policy that grants managerial approval to modifications, and documents all changes thoroughly.]

Security Specifications - The security provisions of a computer system under development must be documented to allow designers to choose the best method of implementation. Appropriate technical, administrative, physical, and personnel security requirements should be specified for the application. Each provision should be specific enough so that appropriate tests can be designed and implemented. Describe the known efforts in this area for this system's development. If there are none, state why.

Design Review and Testing - During the programming stage, specific practices are recommended to enhance the security of the system. These include a peer review of separation of programmers from association with system benefits; redundant computations for error checking; use of high-level languages for compiler error checking, source code and debugging routines; and a careful and thorough testing and evaluation procedure. The results of the design review and testing should be fully documented and maintained in the official agency records. Describe the known efforts in this area for this system's development. If there are none, state why.

Acquisition Specifications - The security requirements of a computer system must be documented to allow decisions in software acquisitions to best accommodate the needs of the system. All provisions should adequately describe the appropriate technical, administrative, physical, and personnel security requirements to provide decision makers with enough specificity to determine whether the requirements will be satisfied by the acquisition or operation of Information Technology Installations or Automated Information Systems. Describe the known efforts in this area for this system's development. If there are none, state why.

Certification/Accreditation - The FIRMR requires that all sensitive systems be certified. Prior to the application being placed into operation, official management authorization needs to be documented. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and that it meets all applicable Federal policies, regulations, standards, and that protection measures appear adequate. If certification/ accreditation documentation is available, attach a copy to this report.

D. Operational Controls

[These are the day-to-day procedures and mechanisms needed to protect the operations of application systems.]

Describe in detail, the following safeguards and whether they are In-Place currently or planned, including dates, for future implementation.

Physical & Environmental Protection - These are measures that minimize interruptions to data processing operations caused by data hardware failures or tampering in the area where processing on the application system takes place.

Production, I/O Controls - These are Input and Output controls for the proper handling, processing, storage, and disposal of input and output media. This also includes access controls (labeling and distribution procedures) on the data and the media.

Emergency, Backup, Disaster Recovery and Contingency Planning - OMB Circular A-130 requires all Federal agencies to develop and maintain appropriate contingency and disaster recovery plans.

> Contingency planning includes workable procedures for continuing to perform essential functions in the event information technology support is interrupted.
>
> Disaster recovery planning includes workable procedures for re-establishing operations at an ADP facility (center).

Audit and Variance Detection - These are controls which allow management to conduct an independent review of records and activities to test the adequacy of controls, and to detect and react to departures from established policies, rules, and procedures. Variance detection for an application checks for anomalies in such items as the numbers and types of transactions, volume and dollar thresholds, and other deviations from standard activity profiles.

Hardware and Software Maintenance Controls - These are controls used to monitor the installation of, and updates to hardware and software to ensure that the software functions as expected. A historical record is to be maintained of all system changes. These controls also may be used to ensure that only authorized software is allowed to reside on the system. These controls may include hardware and system software configuration policy that grants managerial approval to modifications. They may also include products for "virus" protection.

Documentation - Controls in the form of descriptions of the hardware, software, policies, standards, and procedures related to computer security must be fully documented and available.

E. Security Awareness and Training

All employees involved with the management, use, design, development, maintenance and operation of an application should be aware of their security responsibilities and trained in how to fulfill them. A training program that is an integral part of the indoctrination for all new employees should include management's emphasis on security, universal responsibility, data sensitivity, and the effects of security variance on the Department's mission. Other topics may include variance reporting and response, and contingency planning.

F. Technical Controls

[These are hardware and software controls used to provide automated protection.]

User Identification and Authentication - User Identification is a name by which the user is known to the system and is unique, unlikely to change, and need not be kept secret (Users Name). User Authentication or Verification occurs when the individual must pass a further test which "proves" that the user is actually the person associated with the identifier (password). These are controls that identify or verify the eligibility of a station, originator or individual to access specific categories of information. They also perform an activity, or verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authorization/Access Controls - These are controls that may be built into hardware and/or software features that are designed to permit only authorized access to or within the application, to restrict users to transactions and functions, and/or to detect unauthorized activities.

Data Integrity/Validation Controls - These are controls used to protect data from accidental or malicious alteration or destruction, and provide assurance to the user that the data meets an expectation about its quality. Integrity controls refer to administrative procedures which are normally described in vendor-supplied documentation. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements. Data Integrity/Validation Controls involves the examination of computerized data to determine if it is accurate, complete, consistent, unambiguous, and reasonable.

Audit Trails and Journaling - These are controls that provide a transaction monitoring capability with a chronological record of application activities. The process enables reconstruction of a transaction from its inception to final results and may include any modification of files.

Confidentiality Controls - These controls provide protection for data that must be held in confidence and protected from unauthorized disclosure. The controls may provide data protection at the user site, at the computer facility, in transit or a combination of these controls. Under certain circumstances of high risk, data encryption may be needed for the protection of highly sensitive information or personal data covered by the Privacy Act of 1974.

V. ADDITIONAL COMMENTS

[Provide Comments and List Additional Security Needs.]

VI. RECOMMENDATIONS

[Provide specific recommendations that, if implemented, would improve the security posture of this system. These comments should be supplemented by an explanation of the increase in security that should be expected.]